· EL SISTEMA OPERATIVO DE LA CONFIANZA

OmniSec

Confianza, en piloto automático.

Plataforma unificada de Compliance, Inventario de Sistemas y Gestión de Riesgo de Terceros — funcionando de manera continua, no trimestral.

DOCUMENTO PREPARADO POR

NetSec Chile

Representante comercial de OmniSec en Chile

contacto@netsec.cl · +56 2 2306 1000 · WhatsApp +56 9 8776 6273

Avda. Raúl Labbé 13723, of. 404 · Lo Barnechea, Santiago, Chile

01 · QUÉ ES OMNISEC

Una plataforma. Tres frentes críticos.

OmniSec es una plataforma SaaS de **Governance, Risk & Compliance (GRC)** potenciada con inteligencia artificial. Está diseñada para empresas reguladas —sector salud, financiero, infraestructura crítica— que necesitan gestionar múltiples marcos de cumplimiento, mantener un inventario actualizado de sus sistemas críticos, y evaluar continuamente el riesgo de sus proveedores externos.

En lugar de tres herramientas separadas conectadas por planillas Excel, correos y capturas de pantalla, OmniSec consolida los tres frentes en un único registro vivo, que se actualiza automáticamente desde los sistemas que la empresa ya tiene en producción (AWS, Azure, Okta, CrowdStrike, GitHub, Jira, etc.).

EL CICLO OMNISEC	**Mapear una vez. Monitorear siempre. Demostrar cualquier cosa.**

Hechos clave del producto

Modalidad	100% SaaS · nada que instalar · acceso vía navegador
Tiempo de implementación	2 a 4 semanas hasta operar en producción (selección de marco, integraciones, mapeo de políticas, capacitación)
Sector objetivo	Empresas reguladas mid-market y enterprise: salud, finanzas, infraestructura crítica
Tipos de cliente	Usuarios finales · MSSPs · Consultorías · vCISOs
Validación	Más de 1,000 usuarios activos · valoración promedio 5.0
Arquitectura	Cómputo dedicado por tenant · SSO · encriptación extremo a extremo

02 · EL PROBLEMA QUE RESUELVE

Más marcos. Más proveedores. Más auditoría. Mismo personal.

Los equipos de seguridad y cumplimiento enfrentan hoy una presión creciente: SOC 2, ISO 27001, HIPAA, PCI DSS, GDPR, NIS2, DORA, NIST CSF y normas regionales que crecen año a año. A esto se suma la expansión de la lista de proveedores externos —cada uno es una potencial exposición— y la cadencia continua de auditorías, reportes al directorio, y revisiones de seguridad por parte de clientes.

La mayoría de los equipos sigue manejando todo esto con planillas Excel, carpetas compartidas y buena voluntad. El resultado son auditorías de "última hora", brechas que no se ven venir, y riesgo que crece en silencio.

CUMPLIMIENTO

Evidencia recolectada a mano.

Los auditores piden, los ingenieros toman screenshots, los responsables persiguen. La semana antes de la auditoría se convierte en todo el trabajo.

MARCOS

Los mismos controles mapeados de cinco formas distintas.

Cada marco es un proyecto aparte. El solapamiento se resuelve con copy-paste, y queda obsoleto en semanas.

PROVEEDORES

El riesgo vive en otro lugar, o en ninguno.

Una herramienta separada. El inbox de alguien. Un cuestionario de hace 14 meses. La exposición se acumula sin que nadie la vea.

→ **Resultado típico sin OmniSec:** auditorías a las corridas, brechas no detectadas, y riesgo creciendo en silencio.

03 · CÓMO FUNCIONA

Tres pilares. Un flujo continuo.

OmniSec trabaja como un sistema unificado donde los tres pilares se retroalimentan: los controles de cumplimiento se prueban con la evidencia de los sistemas, y los sistemas se evalúan considerando el riesgo de los proveedores que los soportan. Una única fuente de verdad, siempre actualizada.

PILAR 01

Compliance — Mapear cada marco, una sola vez.

Onboarding de todos los marcos que la empresa necesita, lado a lado. Los controles que se solapan entre SOC 2, ISO 27001, HIPAA, PCI DSS, etc. se deduplican automáticamente: **se responde una vez, se cumplen muchos**. La evidencia se recolecta de forma continua desde los sistemas en producción, no en la semana previa al auditor.

PILAR 02

Systems — Una foto viva de qué tiene la empresa y qué la protege.

Inventario completo de sistemas críticos con su clasificación de datos (PCI, PII, tokenizada), su propietario interno, los controles aplicables, y la cobertura real con evidencia. Cuando un sistema cambia, los controles asociados se reevalúan automáticamente. **Se sabe exactamente qué se está protegiendo y con qué cobertura.**

PILAR 03

Vendors — Cada tercero, evaluado de forma continua.

Alta de un proveedor en minutos: OmniSec extrae automáticamente las señales públicas de seguridad (certificaciones, postura TLS, señales de brechas). Cuestionarios inteligentes que los proveedores realmente completan. **El riesgo se ve a nivel de empresa, función y contrato**, y el desvío se detecta el día que cambia — no en la renovación anual.

04 · COBERTURA DE MARCOS

Un mapeo. Todos los marcos.

OmniSec soporta los marcos globales más relevantes y suma regulaciones regionales específicas. Los controles que se solapan entre marcos se deduplican automáticamente, evitando trabajo redundante y inconsistencias.

SOC 2 (Type I & II)	Servicios cloud y B2B SaaS
ISO/IEC 27001	Sistemas de gestión de seguridad de la información (SGSI)
HIPAA	Sector salud y protección de información de pacientes (EE.UU.)
PCI DSS 4.0	Procesamiento y resguardo de datos de tarjetas de pago
NIST CSF / NIST 800-53	Marco de ciberseguridad y controles federales (EE.UU.)
GDPR	Protección de datos personales en la Unión Europea
NIS2	Directiva europea de seguridad de redes y sistemas
DORA	Resiliencia operativa digital para servicios financieros (UE)
CMMC	Cybersecurity Maturity Model Certification (defensa EE.UU.)
FedRAMP	Autorización para proveedores cloud del gobierno federal EE.UU.
ISO 27701 · CSA CCM · SOX ITGC	Privacidad, controles de la nube, controles financieros
+ Regulaciones regionales	Marcos locales según la geografía de operación

→ **Listo para auditoría todos los días**, no solo la semana previa. La evidencia se verifica de forma continua y los gaps se detectan antes de que el auditor los encuentre.

05 · IMPACTO PROBADO

Menos trabajo. Menos riesgo. Una historia más clara.

Estos son los resultados que las organizaciones que ya operan con OmniSec reportan después del primer ciclo completo de uso. Las métricas provienen de la documentación oficial del fabricante.

60–80%

MENOS BÚSQUEDA DE EVIDENCIA

El tiempo que los ingenieros de GRC dedican a recolectar y pegar screenshots se recupera para el trabajo que realmente mejora la postura.

1 equipo

AUDITORÍAS MULTI-MARCO

Ejecutar SOC 2, ISO 27001, HIPAA y PCI como un único programa, no como tres proyectos con tres líderes distintos.

365 días

LISTO PARA AUDITORÍA

Una imagen defendible de la postura de riesgo para el directorio, el auditor y el regulador — no solo la semana previa al trabajo de campo.

2× más rápido

REVISIONES DE SEGURIDAD

Onboarding de proveedores cuando la empresa compra, ciclos de venta cuando la empresa es el proveedor bajo revisión. El mismo registro alimenta ambos lados.

MÉTRICAS ADICIONALES (FUENTE: OMNISEC.COM)

80% reducción en esfuerzo manual · **99.9%** de precisión en cumplimiento · **24/7** verificación continua · **1,000+** usuarios activos · **5.0** valoración promedio

06 · INTEGRACIONES Y SEGURIDAD

Se conecta con lo que ya está en producción.

OmniSec se integra automáticamente con la infraestructura que la empresa ya opera, convirtiéndola en evidencia continua. No requiere agentes ni instalación local: las integraciones usan credenciales con privilegio mínimo y cada sincronización queda registrada.

Integraciones nativas disponibles

Cloud & Infraestructura	AWS · Microsoft Azure · Google Cloud
Identidad y SSO	Okta · Microsoft Entra · Google Workspace
Endpoint & EDR	CrowdStrike · SentinelOne · Microsoft Defender
Repositorios y código	GitHub · GitLab
Colaboración y ticketing	Jira · Slack · Microsoft 365
SIEM & vulnerabilidades	Conectores estándar para los principales SIEM y escáneres
RR.HH. y onboarding	Sistemas de HRIS para evidencia de acceso y bajas
Personalizadas	API y webhooks para integrar herramientas internas

Seguridad de la propia plataforma

- ✓ **Encriptación at-rest y in-transit** — todos los datos cifrados en almacenamiento y tránsito.
- ✓ **Aislamiento por tenant** — los datos de cada organización están completamente aislados del resto.
- ✓ **SSO + MFA + RBAC** — autenticación federada, doble factor y permisos por rol.
- ✓ **Cómputo dedicado** — recursos de procesamiento separados por cliente.
- ✓ **Auditoría completa** — cada acción en la plataforma queda registrada y es trazable.
- ✓ **Privilegio mínimo** — las integraciones usan credenciales con permisos acotados.

07 · PLANES Y PRECIOS

Tres planes. Precio transparente.

OmniSec ofrece tres planes según el tamaño de la organización y la madurez del programa de cumplimiento. **Cada nivel incluye el modelo operativo completo**: sin recargos por marco adicional, sin sorpresas en la implementación, sin aumentos al renovar.

ESSENTIALS	GROWTH	ENTERPRISE
Empresas en crecimiento Lanzando su programa de cumplimiento.	**Mid-market establecido** Programas multi-marco activos.	**Enterprise regulada** Múltiples entidades, geografías o BUs.
Hasta 100 empleados Marcos ilimitados Integraciones estándar Soporte por email	Hasta 300 empleados Marcos ilimitados Integraciones premium (100+) Soporte prioritario + CSM	Usuarios ilimitados Marcos ilimitados Integraciones a medida Soporte dedicado

Lista de precios — Plataforma (USD anual)

Tarifa anual todo-incluido. El primer marco está incluido en el precio base; cada marco adicional se cobra a la tarifa de la banda correspondiente.

Empleados	1 Marco	2 Marcos	3 Marcos	4 Marcos	5 Marcos
1 – 100	$13,800	$18,400	$23,000	$27,600	$32,200
101 – 500	$25,300	$31,050	$36,800	$42,550	$48,300
501 – 2,000	$48,300	$56,350	$64,400	$72,450	$80,500
2,001 – 5,000	$80,500	$92,000	$103,500	$115,000	$126,500
5,000+	*A consultar — contactar al equipo comercial*				

Lista de precios — TPRM (Gestión de Riesgo de Terceros)

Facturado por proveedor bajo gestión. Sin tramos de volumen, sin mínimo, sin setup. Se puede contratar de forma independiente o como módulo de la plataforma.

Proveedores	Cálculo	Costo Anual
10	10 × $230	**$2,300**
25	25 × $230	**$5,750**
50	50 × $230	**$11,500**

100	100 × $230	**$23,000**
250	250 × $230	**$57,500**

08 · PREGUNTAS FRECUENTES

Lo que los clientes suelen preguntar.

¿Qué marcos de cumplimiento soporta OmniSec?

Soporta los principales marcos globales —ISO 27001, SOC 2, HIPAA, GDPR, NIST 800-53, NIST CSF, PCI DSS, NIS2, DORA, CMMC, FedRAMP— y suma marcos regionales según la geografía. Los controles se mapean cruzados entre marcos: el trabajo hecho para un estándar aplica automáticamente a los requisitos solapados de otros.

¿Cómo se asegura la información dentro de OmniSec?

Todos los datos están cifrados at-rest y in-transit. La información de cada organización está aislada de las demás. El acceso se gobierna por roles (RBAC), con SSO y MFA. Cada acción queda registrada en logs. OmniSec aplica a su propia operación el mismo rigor que ayuda a sus clientes a lograr.

¿Cuánto demora la implementación?

La mayoría de las organizaciones está operando en producción en 2 a 4 semanas, lo que incluye selección del marco, integraciones, mapeo de políticas y capacitación del equipo. Es 100% SaaS — no hay nada que instalar localmente.

¿Se puede migrar desde otra herramienta GRC?

Sí. OmniSec soporta importación de políticas, mapeos de controles, registros de riesgo y artefactos de evidencia. El equipo acompaña la transición para que no se pierda información histórica.

¿Cómo se usa la IA en la plataforma?

La IA está embebida en todo el flujo: mapeo de sistemas a controles aplicables, generación de evidencia, detección de desvíos de cumplimiento en tiempo real. No es un chatbot genérico — trabaja sobre el contexto de cumplimiento específico de la empresa.

¿Sirve para organizaciones con múltiples subsidiarias?

Sí. Cada subsidiaria opera su propio espacio de cumplimiento que consolida en una vista unificada a nivel matriz. Las políticas y controles pueden heredarse desde la casa matriz o personalizarse localmente — la sede central tiene visibilidad completa sin limitar la autonomía de cada unidad.

¿Qué soporte se incluye?

Todos los planes incluyen acceso al equipo de soporte. Los planes Growth y Enterprise suman un Customer Success Manager dedicado. La plataforma incluye además un asistente de cumplimiento con IA para consultas del día a día.

09 · PRÓXIMOS PASOS

¿Listo para dejar de perseguir evidencia?

Una conversación de 30 minutos alcanza para entender qué marcos tiene su empresa hoy, qué proveedores está gestionando, y cómo OmniSec se integraría con las herramientas que ya tiene en producción.

01 **Sesión de descubrimiento**
30 minutos. Entendemos su contexto, marcos vigentes, stack tecnológico y prioridades.

02 **Demo personalizada**
45 minutos. Mostramos la plataforma con un caso de uso cercano al suyo. Sin slides genéricos.

03 **Propuesta económica y POC**
Cotización ajustada a su tamaño y alcance. Posibilidad de prueba de concepto antes de comprometerse.

04 **Implementación en 2–4 semanas**
Selección de marco, integraciones, mapeo de políticas, capacitación. Acompañamiento del equipo.

CONTACTO COMERCIAL

NetSec Chile

Representante comercial de OmniSec en Chile

Email: contacto@netsec.cl
Teléfono: +56 2 2306 1000
WhatsApp: +56 9 8776 6273
Dirección: Avda. Raúl Labbé 13723, of. 404
Lo Barnechea, Santiago, Chile